PATENT
29250-002013/US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPELLANTS:	Sarvar PATEL et al.	CONF. NO.:	5912
APPL'N NO.:	10/786,454	GROUP:	2439
FILED:	February 26, 2004	EXAMINER:	Roderick Tolentino
FOR:	METHOD OF GENERATING A CRYPTOSYNC		

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. § 41.37

March 21, 2011

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Mail Stop Appeal Briefs - Patents

Sir/Madam:

Further to Appellants' Notice of Appeal filed December 1, 2010, and the Notice of Panel Decision mailed January 20, 2011, Appellants hereby submit their Brief on Appeal in accordance with 37 C.F.R. § 41.37. The due date of the Appeal Brief is March 21, 2011, as March 20, 2011 is a Sunday.

I. REAL PARTY IN INTEREST.

The real party in interest is Alcatel-Lucent.

II. RELATED APPEALS AND INTERFERENCES.

No related appeals or interferences are known.

III. STATUS OF CLAIMS.

Claims 1-24 are currently pending in the present application. Claims 1 and 24 are independent claims.

Claims 1 and 24 stand finally rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent 7,275,155 to Aull ("Aull") in view of U.S. Patent Publication 2004/0078334 to Malcolm et al. ("Malcolm").

Claims 2-23 stand finally rejected under 35 U.S.C. §103(a) as being unpatentable over Aull in view of Malcolm in further view of U.S. Patent 6,980,658 to Rezaiifar et al. ("Rezaiifar").

Claims 1-24 are being appealed.

IV. STATUS OF AMENDMENTS.

An Amendment under 37 CFR 1.111 was filed on March 1, 2010, with a further Supplemental Amendment filed on April 8, 2010. A Final Office Action was mailed July 1, 2010. No subsequent after-final amendment was filed.

V. SUMMARY OF CLAIMED SUBJECT MATTER.

A. CONCISE EXPLANATION OF THE SUBJECT MATTER SET FORTH IN EACH CLAIM ARGUED SEPARATELY.

1. A GENERAL DISCUSSION OF THE SUBJECT MATTER DESCRIBED IN THE SPECIFICATION TO ASSIST THE BOARD IN UNDERSTANDING EXAMPLE EMBODIMENTS DESCRIBED IN THE PRESENT APPLICATION.

Encryption is used in numerous fields including wireless networks and internet communication. Some encryption algorithms such as DES, AES, etc. involve the use of a key which is a bit sequence used in the encryption algorithm to generate the ciphertext. The encryption key is known at both the send and receive sides of the communication, and at the receive side is used to decrypt the ciphertext into the plaintext.

For example encryption in the wireless communication environment may involve encrypting frames of information sent between a base station and a mobile station. With some encryption schemes, if the same information is encrypted and sent during two different frames, the same ciphertext is produced. This ciphertext can be intercepted by a malicious entity and used by the malicious entity to impersonate another user in what is referred to as a replay attack.

One way to prevent replay attacks is to use cryptosyncs. Cryptosyncs are used in conjunction with encryption and decryption keys. Cryptosyncs have values which change over time so that cipher text generated by an encryption operation changes even when the plain text, which is encrypted, does not.[1]

[1] Spec. at p. 1-2.

Example embodiments provide methods for generating cryptosyncs for use in communications between, for example, two devices.

In wireless communication, mobile stations communicate with base stations over the air. This communication may be encrypted. In CDMA2000, for example, long lived keys such as a cipher key (CK) and an integrity key (IK) associated with a mobile station that are used in the encryption processes and messaging integrity protection processes, respectively. CDMA2000 also provides for, relatively speaking, a long lived cryptosync (e.g., TX_EXT_SSEQ and RX_EXT_SSEQ in CDMA2000). The long-lived cryptosync (LLCS) is used to encrypt and decrypt messages (e.g., signaling messages) between the base station and mobile station, to verify message integrity, or both. After each use, the LLCS is incremented to prevent susceptibility to replay attacks. Initially, upon need or request, the LLCS may be derived using any well-known authentication protocol such as set forth in CDMA2000.[2]

One protocol for data communication between the base station and mobile station, for example, is referred to as the radio link protocol (RLP). To establish an RLP communication, a communication channel between the mobile station and base station is established in a well-known manner such as through message integrity using the LLCS. When the RLP communication ends, the communication channel is torn down. The time during which the communication channel existed for communication of information (e.g., voice, data, etc.) is referred to generally as the communication session. During a communication session, several frames, as defined by the RLP may be communicated. Each frame is encrypted using what

[2] Id. at p. 4-5.

will be referred to hereafter as a short-lived cryptosync (SLCS). The SLCS is short lived in comparison to the LLCS in that the life of the SLCS is limited to the duration of the communication session. A value for the SLCS is newly derived for each communication session.[3]

2. An explanation of the subject matter set forth in each claim argued separately referring to the specification and/or the drawings by reference characters in accordance with 37 C.F.R. § 41.37(c)(1)(v).

i. Claim 1.

Claim 1 recites "A method of generating a cryptosync for a communication session between two communication devices, comprising: deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync". This limitation is supported by at least paragraph [0018][4] of Appellants' specification, herein after referred to as 'the specification', which explains that a first cryptosync, an SLCS, is derived using a portion or the entirety of a second cryptosync, an LLCS.

Claim 1 also recites "the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions." These limitations are supported by at least by at least paragraph

[3] Id. at p. 5-6.
[4] Id. at p. 7, l. 17 -p. 8, l. 4.

[0014][5] of the specification which explains that the time period during which a communication channel exists for communication of information is referred to as a communication session; paragraph [0015][6] of the specification, which explains that the SLCS has a life limited to the duration of a communications session; and paragraph [0016][7] of the specification, which explains that LLCS has a life that extends over multiple communications sessions.

II. Claims 2-4.

Claim 2 depends from claim 1 and recites "wherein the second cryptosync is used for message encryption by at least one of the two devices". Claims 3 and 4 depend from claims 2 and 1, respectively, and recite "wherein the second cryptosync is used for verifying message integrity by at least one of the two devices". These limitations are supported by at least paragraph [0013][8] of the specification which explains that the LLCS is used to encrypt and decrypt messages between a base station and a mobile and/or to verify message integrity.

III. Claim 5

Claims 5 depends from claim 1 and recites "wherein the second cryptosync changes between communication sessions". These limitations are supported by at least paragraph [0017][9] of the specification which explains that the LLCS may be incremented between communications sessions.

[5] Id. at p. 5, l. 15 – p. 6, l. 6.
[6] Id. at p. 6, l. 7 –14.
[7] Id. at p. 6, l. 15 –p. 7, l. 6.
[8] Id. at p. 4, l. 17 –p. 5, l. 14.
[9] Id. at p. 7, l. 7 –16.

IV. CLAIM 6

Claim 6 depends from claim 1 and recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync". This limitation is supported by paragraph [0018][10] of the specification which explains that the SLCS is derived using a portion or the entirety of the LLCS.

V. CLAIM 7

Claim 7 depends from claim 6 and recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence". This limitation is supported by at least Appellants' FIG. 1 and paragraph [0018][11] of the specification which explain that an SLCS may have, for example, 64 bits, 32 bits of which are the LLCS and 32 bits of which are a fixed bit stream.

VI. CLAIM 8

Claim 8 depends from claim 7 and recites "wherein the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence". This limitation is supported by at least Appellants' FIG. 1 and paragraph [0018][12] of the specification which explain that an SLCS may have, for example, 64 bits of which the 32 most significant bits are the LLCS and the 32 least significant bits are a fixed bit stream.

[10] Id. at p. 7, l. 17 –p. 8, l. 4.
[11] Id.
[12] Id.

VII. CLAIM 9

Claim 9 depends from claim 8 and recites "wherein the fixed bit sequence is a string of 0s". This limitation is supported by at least Appellants' FIG. 1 which illustrates the fixed bit sequence occupying the least significant 32 bits of the SLCS being 0s.

VIII. CLAIM 10

Claim 10 depends from claim 8 and recites "wherein the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s". This limitation is supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits of which the 32 most significant bits are the LLCS and the 32 least significant bits are 0s.

IX. CLAIM 11

Claim 11 depends from claim 6 and recites "wherein the deriving step derives a portion of the first cryptosync as the second cryptosync". These limitations are supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits of which the 32 most significant bits are the entire 32 bits of the LLCS. Accordingly, a portion of the first cryptosync is the second cryptosync.

X. CLAIM 12

Claim 12 depends from claim 11 and recites "wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence". This limitation is supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits of which the 32 most significant bits are the LLCS and the 32 least significant bits are a fixed bit sequence, 0s.

XI. CLAIM 13

Claim 13 depends from claim 12 and recites "wherein the fixed bit sequence is a string of 0s". This limitation is supported by at least Appellants' FIG. 1 which illustrates an SLCS having 64 bits of which the 32 most significant bits are the LLCS and the 32 least significant bits are a string of 0s.

XII. CLAIM 14

Claim 14 depends from claim 1 and recites "wherein the deriving step comprises: performing a pseudo-random function on the second cryptosync; and generating the first cryptosync from output of the pseudo-random function." Claim 15 depends from claim 14 and recites "wherein the generating step generates the first cryptosync as the output of the pseudo-random function". These limitations are supported by at least paragraph [0020][13] of Appellants' specification which discuss applying a pseudo random function to the LLCS and using the resulting pseudo-random number as the SLCS.

[13] Id. at p. 8, l. 10-16.

XIII. CLAIMS 16-17

Claim 16 depends from claim 1 and recites "wherein the deriving step is performed at a base station". Claim 17 depends from claim 1 and recites "wherein the deriving step is performed at a mobile station". These limitations are supported by at least paragraph [0022][14] of Appellants' specification which explains that because the LLCS is know at both the mobile station and the bases station, the same SLCS can be derived at both. Further, the same SLCS can be used to encrypt sent information at either the mobile or base station, and to decrypt received data at either the mobile or bases station.

XIV. CLAIMS 18-20

Claim 18 depends from claim 1 and recites "further comprising: encrypting a frame of information to send from the at least one of the two devices using the first cryptosync." Claim 19 depends from claim 18, and recites "wherein the frame of information is a radio link protocol, RLP, frame". Claim 20 depends from claim 18 and recites "further comprising: incrementing the first cryptosync after the encrypting step." These limitations are supported by at least paragraph [0015][15] of Appellants specification which discusses encrypting RLP frames using the SLCS; and paragraph [0022][16] of the specification which discusses encrypting a

[14] Id. at p. 8, l. 21-p. 9, l. 9.
[15] Id. at p. 6, l. 7 -14.
[16] Id. at p. 8, l. 21-p. 9, l. 9.

frame of information at the send side for either the mobile or the base station using the SLCS, and incrementing the SLCS for use in encrypting the next frame.

XV. CLAIMS 21-23

Claim 21 depends from claim 1 and recites "[t]he method of claim 1, further comprising: decrypting a frame of information received at the at least one of the two devices using the first cryptosync." Claim 22 depends from claim 21 and recites "wherein the frame of information is a radio link protocol, RLP, frame". Claim 23 depends from claim 21 and recites "further comprising: incrementing the first cryptosync after the decrypting step." These limitations are supported by at least paragraph [0015][17] of the specification which discusses encrypting RLP frames using the SLCS; and paragraph [0022][18] of the specification which discusses encrypting a frame of information at the send side for either the mobile or the base station using the SLCS, decrypting that same frame of information at the receiving side for either the mobile or the base station using the SLCS, and incrementing the SLCS for use in decrypting the next frame.

XVI. CLAIM 24

Claim 24 recites "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices". This

[17] Id. at p. 6, l. 7 –14.
[18] Id. at p. 8, l. 21-p. 9, l. 9.

limitation is supported by at least paragraph [0018][19] of the specification, which explains that a first cryptosync, the SLCS, is derived using portion or the entirety of the second cryptosync, the LLCS.

Claim 24 also recites "the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions". These limitations are supported by at least paragraph [0014][20] of the specification which explains that the time period during which a communication channel exists for communication of information is referred to as a communication session; paragraph [0015][21] of the specification, which explains that the SLCS has a life limited to the duration of a communications session; and paragraph [0016][22] of the specification, which explains that LLCS has a life that extends over multiple communications sessions.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL.

A. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 1 AND 24 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER U.S. PATENT 7,275,155 TO AULL ("AULL") IN VIEW OF U.S. PATENT PUBLICATION 2004/0078334 TO MALCOLM ET AL. ("MALCOLM").

B. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 2-23 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER AULL IN

[19] Id. at p. 7, l. 17 -p. 8, l. 4.
[20] Id. at p. 5, l. 15 -p. 6, l. 6.
[21] Id. at p. 6, l. 7 -17.
[22] Id. at p. 6, l. 15 -p. 7, l. 6.

VIEW OF MALCOLM IN FURTHER VIEW OF U.S. PATENT 6,980,658 TO REZAIIFAR ET AL. ("REZAIIFAR").

Claims 1-24 are being appealed.

VII. ARGUMENT.

A. APPELLANTS SEEK THE BOARD'S REVIEW OF THE REJECTION OF CLAIMS 1 AND 24 UNDER 35 U.S.C. §103(A) AS BEING UNPATENTABLE OVER U.S. PATENT 7,275,155 TO AULL ("AULL") IN VIEW OF U.S. PATENT PUBLICATION 2004/0078334 TO MALCOLM ET AL. ("MALCOLM").

PRINCIPLES OF LAW

Under 35 U.S.C. §103(a) a patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made (35 U.S.C. §103(a)).

The Examiner bears the initial burden of presenting a *prima facie* case of obviousness in rejecting claims under 35 U.S.C. §103.[23] In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness.[24] In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (1966), *viz.*, (1) the scope and content of the prior art;

[23] *In re Rijckaert*, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993).
[24] *In re Fine*, 837 F.2d 1071, 1073, 5 USPQ2d 1956, 1958 (Fed. Cir. 1988)

(2) the differences between the prior art and the claims at issue; and (3) the level of ordinary skill in the art. Furthermore, "'there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness'...[H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the would employ."[25] Obviousness is then determined on the basis of the evidence as a whole and the relative persuasiveness of the arguments.[26]

ARGUMENTS

In rejecting the above-referenced claims, the July 1, 2010 Final Office Action (hereinafter, " the Final Office Action") asserts the above-referenced claims are obvious in light of the combination of Aull and Malcolm. Appellants respectfully disagree with this assertion.

1. Brief Discussion of Aull and Malcolm

Aull discloses a chain of trust processing system in which a first digital certificate can be used to obtain a second digital certificate. The first certificate can be used to authenticate a user's identity such that a secure channel can be established between a user platform and a server platform. A request for a second certificate can then be forwarded from a user server to a server platform. The server platform then generates the second certificate. The first certificate may be

[25] *KSR Int'l Co. v. Telefax Inc.*, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)).
[26] *See Oetiker*, 977 F. 2d at 1445, 24 USPQ2d at 1444.

a signature certificate and the second certificate may be an encryption certificate. The first certificate may be a signature certificate and the second certificate may be an expiring signature certificate.[27]

Malcolm discloses an information management system including one or more workstations each of which is connected to a network and includes an analyzer, which analyzes data sent from or received at the workstation. The analyzer uses policy data to determine an action to take with respect to the data. These actions can include extracting, checking, or storing digital certificates.[28]

2. The Final Office Action does not identify how each of the limitations of claim 1 are rendered obvious by the cited art.

First, Appellants respectfully submit the Final Office Action has not identified how each of the limitations of claim 1 is taught by the cited art. Appellants note, claim 1 recites "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions". Accordingly, the limitations of claim 1 require a first cryptosync having a life limited to a communications session and a second cryptosync having life extending over multiple communications sessions. Appellants respectfully submit the Final Office Action has not identified how the recited first and second

[27] Aull, Abstract
[28] Malcolm, Abstract

cryptosyncs are taught or rendered obvious by any of the cited art, as is required to establish a *prima facie* case of obviousness.

With respect to the first and second cryptosyncs recited in claim 1, the Final Office Action initially references first and second digital certificates discussed in column 2, lines 63-67 of Aull. In the aforementioned passage, Aull teaches replacing a first, expiring, certificate with a second certificate. Appellants note, on pages 2 and 3 of the final Office Action, the Final Office Action asserts Aull teaches the second digital certificate replacing an "expiring but NOT expired" first digital certificate. Accordingly, Appellants assume the Final Office Action is interpreting the first digital certificate of Aull as corresponding to the recited second cryptosync having a life extending over multiple communications sessions. However, the Final Office Action does not identify what in Aull is considered to be the life of a communications session recited in claim 1. Further, if the first digital certificate of Aull is considered as having a life extending over multiple communications session, the Final Office Action has not identified in Aull, or any other reference, any element corresponding to the recited first cryptosync which has a life **limited to the communication session** as claim 1 requires. For at least this reason, Appellants respectfully submit the Final Office Action has not identified how each of the limitations of claim 1 are taught or rendered obvious by the cited art as is required to support a *prima facie* case of obviousness with respect to claim 1.

Further, the Final Office Action admits Aull fails to teach "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync" as claim 1 recites. With respect to this limitation, the Final Office Action references Malcolm. With respect to the first and second cryptosyncs recited in claim 1, the Final Office Action references a digital certificate and a root certificate, from which the digital certificate may be derived, discussed in paragraph [0145] of Malcolm. Accordingly, Appellants assume the Final Office Action considers the digital certificate and root certificate of Malcolm as corresponding to the recited first and second cryptosync, respectively. However, Appellants respectfully submit the first and second cryptosyncs recited in claim 1 cannot be read upon the digital certificate and root certificate of Malcolm at least because nothing in Malcolm teaches limiting the derived digital certificate to a communication session while using a root certificate for multiple communications sessions as the limitations of claim 1 require of the recited first and second cryptosyncs, respectively. For at least this additional reason, Appellants respectfully submit the Final Office Action has not identified how each of the limitations of claim 1 are taught or rendered obvious by the cited art as is required to support a *prima facie* case of obviousness with respect to claim 1.

Next, Appellants respectfully submit even if, for the sake of argument, the teachings of Aull and Malcom can be interpreted as covering each of the limitations of claim 1, *which Appellants specifically refute above*, the Final Office Action does not identify how the teachings of Malcolm and Aull can be combined or modified to result in a method including each of the limitations of claim 1.

Appellants note the Final Office Action's assertion on page 3 that it would be obvious to use Malcolm's information management system with Aull's chain of trust processing. However, the Final Office Action does not explain how one of ordinary skill in the art would combine or modify these systems in such a way that the limitations of claim 1 are taught. Specifically, Appellants respectfully submit if the systems of Aull and Malcom are combined by being used simultaneously, the combined system would include the second certificate of Aull and the derived digital certificate of Malcolm, both of which the Final Office Action appears to identify as corresponding to the first cryptosync recited in claim 1, as well as the first certificate of Aull and the root certificate of Malcolm, both of which the Final Office Action appears to identify as corresponding to the second cryptosync recited in claim 1. However, the Final Office does not assert that either of the second certificate of Aull and the derived digital certificate of Malcolm, alone, satisfy the requirements of the first cryptosync recited in claim 1. Likewise, the Final Office does not assert that either of the first certificate of Aull and the root digital certificate of Malcolm, alone, satisfy the requirements of the second cryptosync recited in claim 1. Accordingly, combining the systems of Aull and Malcom by simply using the systems together, as the Final Office Action suggests, would not teach the limitations of claim 1.

Appellants further note the Final Office Action includes **no arguments** asserting that it would be obvious to modify any of the first and second certificates taught by Aull or the derived and root certificate taught by Malcolm to teach elements corresponding to either the first or second cryptosync recited in claim 1, nor does the Final Office Action provide a reasoning supporting the conclusion that such modification would be obvious.

Consequently, the Final Office Action provides no interpretation of the systems of Aull and Malcom, alone or in combination, which teaches each of the limitations of claim 1. For at least this additional reason, Appellants respectfully submit the Final Office Action has not identified how each of the limitations of claim 1 are taught or rendered obvious by the cited art as is required to support a *prima facie* case of obviousness with respect to claim 1.

3. The Final Office Action does not articulate a reasoning having a rational underpinning supporting the legal conclusion of obviousness as is required to support a rejection under §103.

Appellants respectfully submit, the Final Office Action does not identify sufficient motivation to combine Aull and Malcolm. As an initial matter, Appellants are aware that the teach-suggest-motivation rationale is not the only rationale which can be used to support an obviousness rejection. However, some rationale is required and aside from identifying an alleged motivation to combine the teachings of Aull and Malcom, the Final Office Action provides no other rationale.

With respect to the reasoning for combining the teachings of Aull and Malcolm, page 3 of the Final Office Action states that it would be obvious to use the system of Malcolm with the system of Aull because it offers the advantage of ensuring that the transmission of data by their staff is always carried out securely, based on benefits discussed in paragraph [0028] of Malcolm.

Appellants respectfully submit, particularly in light of the Final Office Action's failure to articulate how one of ordinary skill in the art would combine or modify either of the systems of Aull and Malcom to achieve a method teaching the limitations of claim 1, as is discussed above in section VII(A)(2) of this Brief, the Final Office Actions' statement regarding motivation to combine the teachings of Aull and Malcom is conclusory and unsupported, and thus, cannot be used to support an obviousness rejection.[29]

Appellants respectfully submit, a person of ordinary skill in the art would have no basis to believe that all possible combinations or modifications regarding the system of Aull based on the teachings of Malcolm would achieve the benefits cited by the Final Office Action. Accordingly, assuming the teachings of Aull can be modified based on the teachings of Malcom, or the that the teachings of Aull and Malcolm can be combined, neither of which Appellants admit, the Final Office Action has provided no support for the assertion that a person of ordinary skill in the art would view this unspecific modification or combination as resulting in achieving the advantages discussed by Malcolm. Accordingly, Appellants respectfully submit, the Final Office Action does not identify a motivation to combine the teachings of Aull and Malcolm. Further, Appellants respectfully submit, the Final Office Action identifies no other rationale supporting the legal conclusion of obviousness.

Consequently, Appellants respectfully submit, the Final Office Action identifies no reasoning having a rational underpinning supporting the legal conclusion of obviousness as is required to support *prima facie* case of obviousness with respect to claim 1.

[29] *KSR Int'l Co. v. Telefax Inc.*, 127 S.Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006))

4. The Final Office Action does not establish a prima facie case of obviousness with respect to claim 24 as is required to support a rejection under §103.

Claim 24 recites "deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions". Page 2 of the Final Office Action indicates claim 24 is rejected for the same reasons as claim 1. Accordingly, for the same reasons discussed above in section VII(A)(2) of this Brief with respect to the rejection of claim 1, Appellants respectfully submit the Final Office Action has not identified how each of the limitations of claim 24 are taught or rendered obvious by the cited art as is required to support a *prima facie* case of obviousness with respect to claim 1. Further, for the same reasons discussed above in section VII(A)(3) of this Brief with respect to the rejection of claim 1, Appellants respectfully submit, the Final Office Action identifies no reasoning having a rational underpinning supporting the legal conclusion of obviousness as is required to support *prima facie* case of obviousness with respect to claim 24.

B. Appellants seek the Board's review of the rejection of Claims 2-23 under 35 U.S.C. §103(a) as being unpatentable over Aull in view of Malcolm in further view of U.S. Patent 6,980,658 to Rezaiifar et al. ("Rezaiifar").

1. Brief Discussion of Rezaiifar.

Rezaiifar discloses a method and apparatus for encrypting transmission in a communication system. Transmission traffic is encrypted on separate protocol layers so that separate encryption elements can be assigned to separate types of transmission traffic. This allows implementation of different types of encryption according to service requirements. Encryption elements use semi-permanent encryption keys with variable cryptosyncs.[30]

2. The Final Office Action does not establish a prima facie case of obviousness with respect to claim 2 as is required to support a rejection under §103.

Claim 2 depends from and thus incorporates the limitations of claim 1. The deficiencies of Aull and Malcom with respect to claim 1 are discussed above. Rezaiifar does not remedy these deficiencies, nor the Examiner rely on Rezaiifar to do so. Accordingly, for at least the reasons discussed above with reference to claim 1, Appellants respectfully submit a *prima facie* case of obviousness has not been established with respect to claim 2.

Further, claim 2 recites "wherein the second cryptosync is used for message encryption by at least one of the two devices". Page 3 of the Final Office Action asserts "Aull and Sunder" fail to teach this limitation. Appellants assume the Final Office Action intended to state that Aull and **Malcom** fail to teach this

[30] Rezaiifar, Abstract.

limitation since Sunder is not used elsewhere in the rejection. Further, the Final Office Action asserts column 3, lines 36-45 of Rezaiifar teach using a crypto sync for message encryption for at least one of the two devices. However, there is no discussion in the Final Office Action regarding how the systems of Aull, Malcom and Rezaiifar would be combined to teach the second crypto sync recited in claim 2 which, according to the limitations of claim 1 and 2, is used to derive the value of first cryptosync, has a lifespan extending multiple communications sessions and is used to encrypt messages by at least one of the two devices. Further, there is no discussion in the Final Office Action regarding how any of the systems of Aull, Malcom and Rezaiifar would be combined or modified to teach an element corresponding to the second crypto sync recited in claim 2.

Accordingly, Appellants respectfully submit the Final Office Action has not identified how each of the limitations of claim 2 are taught or rendered obvious by the cited art as is required to support a *prima facie* case of obviousness with respect to claim 1.

3. The Final Office Action does not establish a prima facie case of obviousness with respect to any of claims 3-23 as is required to support a rejection under §103.

First, Appellants note, for each of the rejections of claims 3-23, no reasoning is provided supporting the conclusion that it would be obvious to combine Aull, Malcom and Rezaiifar in such a way that the limitations of the claim are taught. For at least this reason, Appellants respectfully submit a *prima* *facie* case of obviousness has not been established with respect to any of claims 3-23.

Next, Appellants note, the Final Office Action may intend to apply the same reasoning regarding obviousness discussed with respect to claim 2 to each of claims 3-23. However, if this is the case, Appellants respectfully submit, for each of the rejections of claims 3-23, there is no discussion in the Final Office Action regarding how the systems of Aull, Malcolm and Rezaiifar would be combined to teach the limitations of any of claims 3-23. Further, there is no discussion in the Final Office Action regarding how any of the systems of Aull, Malcom and Rezaiifar would be modified to teach the limitations of any of claims 3-23.

Accordingly, Appellants respectfully submit the Final Office Action has not identified how each of the limitations of any of claims 3-23 are taught or rendered obvious by the cited art as is required to support a *prima facie* case of obviousness with respect to claims 3-23.

Further, Appellants respectfully submit the Final Office Action does not identify how the following limitations are taught by the cited art.

Claim 6

Claim 6 recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync". With respect to this limitation, the Final Office Action references column 2, lines 25-38 of Rezaiifar. However, the cited portion of Rezaiifar discusses only one cryptosync, not deriving a first cryptosync as at least a portion of a second cryptosync. Accordingly, the Final

Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 6.

Claim 7

Claim 7 recites "wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence". The Final Office Action asserts this limitation is taught by column 4, lines 46-62 of Rezaiifar. The cited portion of Rezaiifar discusses using an ENC-SEQ generator to provide a sequence number used to construct a crypto sync. Appellants assume the Final Office Action is interpreting the generated sequence as corresponding to the recited fixed bit sequence. However, the Final Office Action does not identify what in Rezaiifar is being considered as corresponding to the recited second cryptosync. Accordingly, the Final Office Action does not identify how the cited art, alone or in combination, teaches a cryptosync having a portion of the second crypto sync **and** a fixed bit sequence. Accordingly, the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 7.

Claim 8

Claim 8 recites "wherein the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence". With respect to these limitations, the Final Office Action again points to column 4, lines 46-62 of Rezaiifar. However, for the same reasons discussed above with reference to claim

7, Appellants respectfully submit the Final Office Action does not identify how the cited art, alone or in combination, teaches a cryptosync having a portion of the second crypto sync **and** a fixed bit sequence. Accordingly, the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 8.

Claim 9

Claim 9 recites "wherein the fixed bit sequence is a string of 0s". With respect to this limitation the Final Office Action references an EID value discussed in column 9, lines 11-22 of Rezaiifar. However, Appellants respectfully submit the EID bit 807 discussed in the portion of Rezaiifar referenced by the Final Office Action is a single bit, not a string of 0s. Further, the EID bit 807 is included in a frame 800 which is not taught by Rezaiifar as being a cryptosync as claim 9 requires. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 9.

Claim 10

Claim 10 recites "wherein the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s". With respect to these limitations the Final Office Action again references an EID value discussed in column 9, lines 11-22 of Rezaiifar. However, as is discussed above, the EID bit

807 discussed in the portion of Rezaiifar referenced by the Final Office Action is a single bit, not a string of 32 0s. Further, the EID bit 807 is included in a frame 800 which is not taught by Rezaiifar as being a cryptosync. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 10.

Claim 11

Claim 11, recites "wherein the deriving step derives a portion of the first cryptosync as the second cryptosync". Similar to claim 6, with respect to this limitation of claim 11, the Final Office Action references column 2, lines 25-38 of Rezaiifar. However, as is discussed above, the cited portion of Rezaiifar discusses only one cryptosync, not deriving a first cryptosync as a portion of a second cryptosync. Accordingly, the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 11.

Claim 12

Claim 12 recites "wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence". Similar to claim 7, in rejecting claim 12, the Final Office Action asserts this limitation is taught by column 4, lines 46-62 of Rezaiifar. However, as is discussed above with reference to claim 7, the cited portion of Rezaiifar discusses using a ENC-SEQ generator to provide a sequence number used to construct a crypto sync. Appellants assume the Final Office Action is interpreting the generated sequence as corresponding to the recited fixed bit sequence. However, the Final Office Action does not identify what in Rezaiifar is being considered as corresponding to the recited second cryptosync. Accordingly, the Final Office Action does not identify how the cited art, alone or in combination, teaches a cryptosync having a portion of the second crypto sync **and** a fixed bit sequence. Accordingly, the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 12.

Claim 13

Claim 13 recites "wherein the fixed bit sequence is a string of 0s". With respect to this limitation, the Final Office Action again identifies the EID value discussed in column 9, lines 11-22 of Rezaiifar. However, as is discussed above with respect to claim 10, the EID bit 807 discussed in the portion of Rezaiifar referenced by the Final Office Action is a single bit, not a string of 32 0s. Further, the EID bit 807 is included in a frame 800 which is not taught by Rezaiifar as being a cryptosync. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 13.

Claims 16 and 17

Claim 16 recites "wherein the deriving step is performed at a base station" and claim 17 recites "wherein the deriving step is performed at a mobile station". With respect to each of these limitations, the Final Office Action references column 3, lines 36-45 of Rezaiifar. The portion of Rezaiifar referenced by the Final Office Action discusses a CDMA wireless telephone system which generally includes mobile subscriber units 12 and base stations 14. Appellants assume the Final Office Action is identifying the mobile subscriber units 12 and base station 14 as corresponding to the base station recited in claim 16 and the mobile station recited in claim 17. However, there is no discussion of performing the operation of deriving a cryptosync at either the base station or the mobile station in the portion of Rezaiifar referenced by the Final Office Action. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of either of claims 16 and 17.

Claim 18

Claim 18 recites "encrypting a frame of information to send from the at least one of the two devices using the first cryptosync". With respect to this limitation the Final Office Action references column 2, lines 19-23 of Rezaiifar which discusses encrypting transmission traffic. However, there is no discussion in the Final Office Action of what in this portion of Rezaiifar is being considered as corresponding to the first cryptosync recited in claim 18, nor is there any discussion of how Aull, Malcom and Rezaiifar are being interpreted as teaching a first cryptosync meeting all the requirements of claim 1 which is used to encrypt a frame of information as the limitations of claim 18 require. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 18.

Claim 20

Claim 20 recites "incrementing the first cryptosync after the encrypting step". With respect to this limitation the Final Office Action references column 2, lines 38-48 of Rezaiifar, which teach incrementing a cryptosync value at a receiving end and a transmission end. However, claim 20 depends from claim 1 and the Final Office Action does not identify how Rezaiifar teaches the cryptosync mentioned in the passage of referred to by the Final Office Action being derived based on the value of a second cryptosync as claim 1 requires. Further, there is no discussion of how any of Aull, Malcom and Rezaiifar are being modified or combined to teach incrementing a cryptosync value corresponding to the first cryptosync recited in claim 1 as the limitations of claim 20 require. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 20.

Claim 21

Claim 21 recites "decrypting a frame of information received at the at least one of the two devices using the first cryptosync". With respect to this limitation the Final Office Action references column 5, lines 56-67 of Rezaiifar which decryption/encryption at a physical layer. However, there is no discussion of cryptosyncs in the portion of Rezaiifar referenced by the Final Office Action. Further, claim 21 depends from claim 1, and the Final Office Action does not identify where Rezaiifar teaches the encryption/decryption mentioned in the passage of referred to by the Final Office Action being performed using a cryptosync derived based on the value of a second cryptosync as claim 1 requires. Additionally, there is no discussion of how any of Aull, Malcom and Rezaiifar are being modified or combined to teach decrypting a frame of information received at the at least one of the two devices using a cryptosync value corresponding to the first cryptosync recited in claim 1 as the limitations of claim 21 require. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 21.

Claim 23

Claim 23 recites "incrementing the first cryptosync after the decrypting step". With respect to this limitation the Final Office Action references column 2, lines 38-48 of Rezaiifar which teach incrementing a crypto sync value at a receiving end and a transmission end. However, claim 23 depend from claim 1 and the Final Office Action does not identify where Rezaiifar teaches the cryptosync mentioned in the passage referred to by the Final Office Action being derived based on the value of a second cryptosync as claim 1 requires. Further, there is no discussion of how any of Aull, Malcom and Rezaiifar is being modified or combined to teach incrementing a cryptosync value corresponding to the first cryptosync recited in claim 1 as the limitations of claim 20 require. Accordingly, Appellants respectfully submit the Final Office action does not identify how Rezaiifar, or any of the other cited art, alone or in combination, teaches the limitations of claim 23.

VIII. CONCLUSION.

In light of the foregoing arguments, Appellants respectfully request the Board to reverse the Final Office Action's rejections of claims 1-24.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY & PIERCE, PLC

By JHA Reg No. 64,371
Gary D. Yacura, Reg. No. 35,416

GDY/JHA:eaf

P.O. Box 8910
Reston, VA 20195
(703) 668-8000

IX. CLAIMS APPENDIX.

Claims on Appeal:

1. (Previously Presented) A method of generating a cryptosync for a communication session between two communication devices, comprising:

deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions.

2. (Original) The method of claim 1, wherein the second cryptosync is used for message encryption by at least one of the two devices.

3. (Original) The method of claim 2, wherein the second cryptosync is used for verifying message integrity by at least one of the two devices.

4. (Original) The method of claim 1, wherein the second cryptosync is used for verifying message integrity by at least one of the two devices.

5. (Original) The method of claim 1, wherein the second cryptosync changes between communication sessions.

6. (Original) The method of claim 1, wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync.

7. (Original) The method of claim 6, wherein the deriving step derives the first cryptosync as at least a portion of the second cryptosync and a fixed bit sequence.

8. (Original) The method of claim 7, wherein the deriving step derives most significant bits of the first cryptosync as the portion of the second cryptosync and derives least significant bits of the first cryptosync as the fixed bit sequence.

9. (Original) The method of claim 8, wherein the fixed bit sequence is a string of 0s.

10. (Original) The method of claim 8, wherein the deriving step derives a 32 most significant bits of the first cryptosync as the second cryptosync and derives a 32 least significant bits of the first cryptosync as a string of 0s.

11. (Original) The method of claim 6, wherein the deriving step derives a portion of the first cryptosync as the second cryptosync.

12. (Original) The method of claim 11, wherein the deriving step derives a first portion of the first cryptosync as the second cryptosync and derives a second portion of the first cryptosync as a fixed bit sequence.

13. (Original) The method of claim 12, wherein the fixed bit sequence is a string of 0s.

14. (Original) The method of claim 1, wherein the deriving step comprises:

performing a pseudo-random function on the second cryptosync; and

generating the first cryptosync from output of the pseudo-random function.

15. (Original) The method of claim 14, wherein the generating step generates the first cryptosync as the output of the pseudo-random function.

16. (Original) The method of claim 1, wherein the deriving step is performed at a base station.

17. (Original) The method of claim 1, wherein the deriving step is performed at a mobile station.

18. (Original) The method of claim 1, further comprising:

encrypting a frame of information to send from the at least one of the two devices using the first cryptosync.

19. (Original) The method of claim 18, wherein the frame of information is a radio link protocol, RLP, frame.

20. (Original) The method of claim 18, further comprising:

incrementing the first cryptosync after the encrypting step.

21. (Original) The method of claim 1, further comprising:

decrypting a frame of information received at the at least one of the two devices using the first cryptosync.

22. (Original) The method of claim 21, wherein the frame of information is a radio link protocol, RLP, frame.

23. (Original) The method of claim 21, further comprising:

incrementing the first cryptosync after the decrypting step.

24. (Previously Presented) A method of generating a cryptosync for a communication session between two communication devices, comprising:

deriving, at a network element, a value of a first cryptosync for the communication session based on a value of a second cryptosync used to encrypt further communication between the two devices, the first cryptosync having a life limited to the communication session, the communication session being defined as a period of time a channel for communication exists between the two communication devices, the second cryptosync having a life extending over multiple communication sessions.

X. EVIDENCE APPENDIX.

None.

XI. RELATED PROCEEDINGS APPENDIX.

None.